PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

To:

United States Patent and Trademark Office
(Box PCT)
Crystal Plaza 2
Washington, DC 20231
ÉTATS-UNIS D'AMÉRIQUE

in its capacity as elected Office

Date of mailing (day/month/year) 12 March 1999 (12.03.99)	
International application No. PCT/DE98/01922	**Applicant's or agent's file reference** T97014 PCT
International filing date (day/month/year) 10 July 1998 (10.07.98)	**Priority date** (day/month/year) 10 July 1997 (10.07.97)
Applicant MARINGER, Günter et al	

1. The designated Office is hereby notified of its election made:

[X] in the demand filed with the International Preliminary Examining Authority on:

09 February 1999 (09.02.99)

[ ] in a notice effecting later election filed with the International Bureau on:

2. The election [X] was

[ ] was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO **34, chemin des Colombettes** **1211 Geneva 20, Switzerland**	Authorized officer Diana Nissen
Facsimile No.: (41-22) 740.14.35	Telephone No.: (41-22) 338.83.38

PATENT COOPERATION TREATY

From the
INTERNATIONAL PRELIMINARY EXAMINING AUTHORITY

To:
RIEBLING, Peter
Postfach 3160
D-88113 Lindau
GERMANY

PCT

NOTIFICATION OF RECEIPT OF INTERNATIONAL PRELIMINARY EXAMINATION DEMAND

(PCT Rules 59.3 e) and 61.1 b), first sentence, and PCT administrative instruction section 601) a))

	Date of mailing *(day/month/year)* 25.02.99
Applicant's or agent's file reference 12343.3-D1461	IMPORTANT NOTIFICATION

International application No. PCT/DE98/01922	International filing date *(day/month/year)* 10/07/1998	Priority date *(day/month/year)* 10/07/1997

Applicant
DETEMOBIL DEUTSCHE TELEKOM MOBILNET GMBH et al.

1. This applicant is hereby notified that this International Preliminary Examining Authority considers the following date to be the date of receipt of the demand for international preliminary examination of the international application:

09/02/1999

2. This date of receipt is

☒ the actual date of receipt of the demand at the Authority (Rule 61.1.b)).
☐ the actual date on which the demand was accepted on behalf of the Authority (Rule 59.3 e))
☐ the date on which the amendments, if any, to be made to the demand have been received by the Authority in response to a request to remove the defects in the demand (Form PCT/IPEA/404)).

3. ☐ **Note:** The date of receipt is **AFTER** the expiration of a period of 19 months from the priority date. Consequently, the election(s) made in the demand do not defer entry into the national phase until 30 months after the priority date (or later in some Offices) (Article 39.1). The acts to be performed for entering the national phase must be done within 20 months from the priority date (or later in some Offices) (Article 22). For more information, see Volume II of the PCT Applicant's Guide.

☐ *(if applicable)* This Notification confirms the information given by telephone or fax or in person on:

4. In the case given in paragraph 3, a copy of this Notification has been sent to the International Bureau.

Name and mailing address of the IPEA/ European Patent Office D-80298 Munich Tel. (+ 49-89) 2399-0, Tx: 523656 epmu d Fax: (+ 49-89) 2399-4465	Authorized officer: Doris Jäger (signature) Telephone No. – 2564

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

24

Absender: DIE MIT DER INTERNATIONALEN VORLÄUFIGEN PRÜFUNG BEAUFTRAGTE BEHÖRDE

PCT

An
RIEBLING, Peter
Postfach 3160
D-88113 Lindau
ALLEMAGNE

Vorlage | Ablage D1461
Haupttermin
Eing.: 26.FEB.1999
PA. Dr. Peter Riebling
Bearb.: | Vorgelegt.

MITTEILUNG ÜBER DEN EINGANG DES ANTRAGS BEI DER ZUSTÄNDIGEN MIT DER INTERNATIONALEN VORLÄUFIGEN PRÜFUNG BEAUFTRAGTEN BEHÖRDE

(Regeln 59.3 e) und 61.1 b) Satz 1 PCT sowie Abschnitt 601 a) der Verwaltungsvorschriften)

Absendedatum (Tag/Monat/Jahr)	25.02.99
Aktenzeichen des Anmelders oder Anwalts: 12343.3-D1461	WICHTIGE MITTEILUNG

Internationales Aktenzeichen	Internationales Anmeldedatum (Tag/Monat/Jahr)	Prioritätsdatum (Tag/Monat/Jahr)
PCT/DE 98/ 01922	10/07/1998	10/07/1997

Anmelder: DETEMOBIL DEUTSCHE TELEKOM MOBILNET GMBH et al.

1. Dem Anmelder wird mitgeteilt, daß die mit der internationalen vorläufigen Prüfung beauftragte Behörde nachstehendes Datum als Eingangsdatum des Antrags auf internationale vorläufige Prüfung der internationalen Anmeldung betrachtet:

09/02/1999

2. Dieses Eingangsdatum entspricht:

☒ dem tatsächlichen Eingangsdatum des Antrags bei der Behörde (Regel 61.1 b)).

☐ dem tatsächlichen Datum, an dem der Antrag für die Behörde entgegengenommen worden ist (Regel 59.3 e)).

☐ dem Datum, an dem die Behörde auf die Aufforderung zur Behebung von Mängeln des Antrags (Formblatt PCT/IPEA/404) hin die erforderlichen Berichtigungen erhalten hat.

3. ☐ ACHTUNG: Das Eingangsdatum liegt NACH dem Ablauf von 19 Monaten ab dem Prioritätsdatum. Folglich führt die im Antrag erfolgte Auswahl von Vertragsstaaten nicht zu einer Verschiebung des Eintritts in die nationale Phase bis zu 30 (oder in manchen Ämtern mehr) Monaten ab dem Prioritätsdatum (Artikel 39 (1)). Daher müssen die für den Eintritt in die nationale Phase erforderlichen Handlungen innerhalb von 20 (oder in manchen Ämtern mehr) Monaten ab dem Prioritätsdatum (Artikel 22) vorgenommen werden. Nähere Einzelheiten sind dem *PCT-Leitfaden für Anmelder*, BAND II zu entnehmen.

☐ *(falls zutreffend)* Diese Mitteilung gilt als Bestätigung der am _____ per Telefon, Fax oder persönlich erteilten Auskunft.

4. Nur wenn Punkt 3 zutrifft, wurde dem Internationalen Büro ein Exemplar dieser Mitteilung übermittelt.

Name und Postanschrift der mit der internationalen vorläufigen Prüfung beauftragten Behörde	Bevollmächtigter Bediensteter
Europäisches Patentamt D-80298 München Tel. (+49-89) 2399-0, Tx 523656 epmu d Fax (+49-89) 2399-4465	Doris Jäger Tel. -2564

Formblatt PCT/IPEA/402 (Juli 1998) P20454 (22/02/1999)

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

(Artikel 36 und Regel 70 PCT)

18

Aktenzeichen des Anmelders oder Anwalts	WEITERES VORGEHEN	siehe Mitteilung über die Übersendung des internationalen vorläufigen Prüfungsbericht (Formblatt PCT/IPEA/416)
12343.3-D1461		
Internationales Aktenzeichen	Internationales Anmeldedatum *(Tag/Monat/Jahr)*	Prioritätsdatum *(Tag/Monat/Tag)*
PCT/DE98/01922	10/07/1998	10/07/1997
Internationale Patentklassification (IPK) oder nationale Klassifikation und IPK		
H04L9/32		
Anmelder		
DETEMOBIL DEUTSCHE TELEKOM MOBILNET GMBH et al.		

1. Dieser internationale vorläufige Prüfungsbericht wurde von der mit der internationale vorläufigen Prüfung beauftragte Behörde erstellt und wird dem Anmelder gemäß Artikel 36 übermittelt.

2. Dieser BERICHT umfaßt insgesamt 5 Blätter einschließlich dieses Deckblatts.

   ☒ Außerdem liegen dem Bericht ANLAGEN bei; dabei handelt es sich um Blätter mit Beschreibungen, Ansprüchen und/oder Zeichnungen, die geändert wurden und diesem Bericht zugrunde liegen, und/oder Blätter mit vor dieser Behörde vorgenommenen Berichtigungen (siehe Regel 70.16 und Abschnitt 607 der Verwaltungsrichtlinien zum PCT).

   Diese Anlagen umfassen insgesamt 4 Blätter.

3. Dieser Bericht enthält Angaben zu folgenden Punkten:

   - I ☒ Grundlage des Berichts
   - II ☐ Priorität
   - III ☐ Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit
   - IV ☐ Mangelnde Einheitlichkeit der Erfindung
   - V ☒ Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderische Tätigkeit und der gewerbliche Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung
   - VI ☐ Bestimmte angeführte Unterlagen
   - VII ☐ Bestimmte Mängel der internationalen Anmeldung
   - VIII ☐ Bestimmte Bemerkungen zur internationalen Anmeldung

Datum der Einreichung des Antrags	Datum der Fertigstellung dieses Berichts
09/02/1999	09.09.99
Name und Postanschrift der mit der internationalen vorläufigen Prüfung beauftragten Behörde: Europäisches Patentamt D-80298 München Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Bevollmächtigter Bediensteter: Snell, T Tel. Nr. +49 89 2399 8802

Formblatt PCT/IPEA/409 (Deckblatt) (Januar 1994)

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

Internationales Aktenzeichen PCT/DE98/01922

I. Grundlage des Berichts

1. Dieser Bericht wurde erstellt auf der Grundlage (*Ersatzblätter, die dem Anmeldeamt auf eine Aufforderung nach Artikel 14 hin vorgelegt wurden, gelten im Rahmen dieses Berichts als "ursprünglich eingereicht" und sind ihm nicht beigefügt, weil sie keine Änderungen enthalten.)*:

Beschreibung, Seiten:

2-10	ursprüngliche Fassung			
1	eingegangen am	21/08/1999	mit Schreiben vom	19/08/1999

Patentansprüche, Nr.:

1-14	eingegangen am	21/08/1999	mit Schreiben vom	19/08/1999

Zeichnungen, Blätter:

1/1	ursprüngliche Fassung

2. Aufgrund der Änderungen sind folgende Unterlagen fortgefallen:

   ☐ Beschreibung, Seiten:
   ☐ Ansprüche, Nr.:
   ☐ Zeichnungen, Blatt:

3. ☐ Dieser Bericht ist ohne Berücksichtigung (von einigen) der Änderungen erstellt worden, da diese aus den angegebenen Gründen nach Auffassung der Behörde über den Offenbarungsgehalt in der ursprünglich eingereichten Fassung hinausgehen (Regel 70.2(c)):

4. Etwaige zusätzliche Bemerkungen:

V. Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Feststellung

Neuheit (N)	Ja:	Ansprüche	1-14
	Nein:	Ansprüche	
Erfinderische Tätigkeit (ET)	Ja:	Ansprüche	1-14
	Nein:	Ansprüche	
Gewerbliche Anwendbarkeit (GA)	Ja:	Ansprüche	1-14
	Nein:	Ansprüche	

2. Unterlagen und Erklärungen

siehe Beiblatt

Zu Punkt V

Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Die Erfindung betrifft ein Verfahren (Anspruch 1) und eine Vorrichtung (Anspruch 14) zur gegenseitigen Authentisierung von Komponenten in einem Netz.

2. Stand der Technik ist das sogenannte "Challenge-Response-Verfahren" (siehe D1), bei dem von der authentisierenden Komponente (das Netz) eine Zufallszahl ("Challenge") an die zu authentisierende Komponente (eine Mobilstation) gesandt wird, die mit Hilfe eines Algorithmus und eines geheimen Schlüssels in eine Antwort ("Response") umgerechnet wird. Im Netz wird mit gleichem Schlüssel und dem gleichen Algorithmus die erwartete Antwort errechnet, und als Datenpaar an das Netz aufgrund einer Anforderung übermittelt. Eine Übereinstimmung beweist die Echtheit der Mobilstation. Das Verfahren wird in der umgekehrten Richtung wiederholt, um das Netz zu authentisieren.

   Es ist ferner bekannt, den Algorithmus und den Schlüssel in einem zentralen Authentisierungszentrum zu verwalten, wobei an das Netz zum Zwecke der Authentisierung Challenge/Response-Paare im voraus übertragen werden.

3. Bei dieser zentralen Verwaltung ergibt sich bei der Authentisierung des Netzes das Problem, daß die Antwort zu der von der Mobilstation gesendeten Challenge nur in dem Authentisierungszentrum errechnet werden kann, was zu einer Verzögerung führt.

4. Gemäß der Erfindung wird dieses Problem gelöst, indem die von der Mobilstation an das Netz gesendete Antwort gleich als Zufallszahl ("Challenge 2") für das Netz verwendet wird; da das Netz bereits diese Zahl kennt, kann die darauf basierende Antwort ("Response 2") bereits im voraus vom Authentisierungszentrum angefordert werden. So wird der Authentisierungsvorgang deutlich beschleunigt.

   Da weder das Problem noch die Lösung aus D1 bekannt oder in naheliegender Weise ableitbar sind, erfüllt der Anspruch 1 die Erfordernisse der Artikel 33(1)-(3)

PCT.

5. Die Ansprüche 2-14 sind abhängig vom Anspruch 1 und erfüllen daher ebenfalls die Erfordernisse der Artikel 33(1)-(3) PCT.

Verfahren und Vorrichtung zur gegenseitigen Authentisierung von Komponenten in einem Netz mit dem Challenge-Response-Verfahren.

Die Erfindung betrifft ein Verfahren und eine Vorrichtung zur gegenseitigen Authentisierung von Komponenten in einem Netz mit dem Challenge-Response-Verfahren nach dem Oberbegriff des Anspruches 1. Insbesondere betrifft die Erfindung die gegenseitige Authentisierung eines Endgeräts, bevorzugt einer Mobilstation gegenüber dem Netz und umgekehrt. Im folgenden wird der Begriff „Mobilstation" verwendet; dies ist nicht einschränkend zu verstehen. Hierunter sollen alle möglichen Endgeräte fallen, auch stationäre, wie z.B. einzelne Nutzer eines Computers in einem drahtgebundenen System.

Authentisieren dient zur Überprüfung der Echtheit der zu authentisierenden Komponente.
Stand der Technik ist das sogenannte Challenge-Response-Verfahren: Bei diesem wird von der authentisierenden Komponente (N = Netz) eine Zufallszahl (Challenge) an die zu authentisierende Komponente (M = Mobilstation) gesandt, die mit Hilfe eines Algorithmus (A) und eines geheimen, beiden Komponenten bekannten Schlüssels K in eine Antwort (Response) umgerechnet wird. Im Netz N wird mit gleichem Schlüssel K und dem gleichen Algorithmus A die erwartete Response errechnet; eine Übereinstimmung der von M zurückgesendeten mit der bei N errechneten Response beweist die Echtheit von M.
Eine gegenseitige Authentisierung wird nach Stand der Technik dadurch erreicht, daß der obige Ablauf mit umgekehrter Rollenverteilung stattfindet. Eine derartige bidirektionale Authentisierung ist z.B. in der EP-A-0 447 380 beschrieben.

Bei dem bekannten Challenge-Response-Verfahren gibt demnach das Festnetz eine Challenge an die Mobilstation M und die

Patentansprüche

1. Verfahren zur gegenseitigen Authentisierung von Komponenten in einem Netz nach dem Challenge-Response-Verfahren, bei dem zur Authentifizierung eines Endgeräts (M), insbesondere einer Mobilstation, gegenüber dem Netz das Netz (N) von einem Authentisierungszentrum (AUC) aufgrund einer Anforderung mindestens ein Datenpaar bestehend aus einer ersten Zufallszahl (Challenge 1) und einer ersten Antwort (Response 1) anfordert und die erste Zufallszahl (Challenge 1) an das Endgerät (M) weiterleitet, welches aufgrund eines intern gespeicherten Schlüssels (Ki) hieraus ebenfalls die erste Antwort (Response 1) berechnet und an das Netz (N) sendet, wobei ferner eine Authentisierung des Netzes (N) gegenüber dem Endgerät (M) stattfindet, indem das Endgerät eine zweite Zufallszahl (Challenge 2) zum Netz sendet, die vom Netz mit einer im AUC berechneten zweiten Antwort (Response 2) beantwortet wird, **dadurch gekennzeichnet,**
daß die vom Endgerät (M) an das Netz (N) gesendete erste Antwort (Response 1) gleichzeitig als zweite Zufallszahl (Challenge 2) verwendet wird, wobei vom Netz die zweite Antwort (Response 2) bereits zuvor zusammen mit der ersten Zufallszahl und der ersten Antwort im Rahmen eines Dreier-Datensatzes (Challenge 1/ Response 1/ Response 2) vom AUC angefordert wurde.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet,** daß das Netz die von dem Endgerät (M) zurückgesandte erste Antwort (Response 1) als zweite Zufallszahl (Challenge 2) interpretiert.

3. Verfahren nach Anspruch 1 oder 2, **dadurch gekennzeichnet, daß** die Übertragung der ersten Zufallszahl (Challenge 1) und ersten Antwort (Response 2) von dem Netz (N) zu dem Endgerät (M) zeitlich hintereinander folgend erfolgt.

4. Verfahren nach Anspruch 1 oder 2, **dadurch gekennzeichnet,** daß die Übertragung des Datenpaares (Challenge 1/Response 2) von dem Netz (N) zu dem Endgerät (M) gleichzeitig in Form eines einzigen Datensatzes erfolgt.

5. Verfahren nach einem der Ansprüche 2, 3 oder 4, **dadurch gekennzeichnet, daß** das Netz Datensätze vom Authentifizierungszentrum (AUC) in Form von Dreier-Datensätzen (Challenge 1/Response 1/Response 2) anfordert.

6. Verfahren nach Anspruch 5, dadurch gekennzeichnet, daß zur Herabsetzung der Anforderungshäufigkeit mehrere Dreier-Datensätze vom AUC als Vorrat geliefert werden.

7. Verfahren nach Anspruch 4 oder 5, **dadurch gekennzeichnet, daß** zur Verwendung der ersten Antwort (Response 1) des Endgeräts (M) als zweite Zufallszahl (Challenge 2) zwecks Authentifikation des Netzes gegenüber dem Endgerät (M) die kürzere Länge der ersten Antwort (Response 1) auf die größere Länge der zweiten Zufallszahl (Challenge 2) aufgefüllt wird.

8. Verfahren nach Anspruch 7, **dadurch gekennzeichnet, daß** das Auffüllen teilnehmer-individuell erfolgt und daß die vollständige Länge der ersten Antwort (Response 1) vor der Übertragung auf die Gegenstelle verkürzt wird.

9. Verfahren nach Anspruch 8, **dadurch gekennzeichnet, daß** die ersten Antwort (Response 1) mit definierten Bits aus dem

geheimen Schlüssel (Ki) auf die Länge der zweiten Zufallszahl (Challenge 2) aufgefüllt wird.

10. Verfahren nach Anspruch 8, **dadurch gekennzeichnet**, daß die zweite Zufallszahl (Challenge) der originalen ersten Antwort (Response 1) vor ihrer Kürzung entspricht.

11. Verfahren nach einem der Ansprüche 1 - 10, **dadurch gekennzeichnet**, daß das Netz ein GSM-Netz ist.

12. Verfahren nach einem der Ansprüche 1 - 10, **dadurch gekennzeichnet**, daß das Netz ein drahtgebundenes Netz ist.

13. Verfahren nach Anspruch 12, **dadurch gekennzeichnet**, daß die einzelnen, sich gegenseitig authentisierenden Komponenten in einem drahtgebundenen Netz verschiedene Kontrolleinheiten von Computern sind, welche sich gegenüber einem Zentralcomputer authentifizieren und umgekehrt.

14. Verfahren nach einem der Ansprüche 1 - 13, **dadurch gekennzeichnet**, daß das AUC die vom Netz geforderten Dreier-Datensätze berechnet und diese auf Anforderung vom Netz Off-Line und zeitlich unabhängig, jedoch auf jeden Fall vor dem Datenaustausch zwischen Netz und Endgerät an das Netz übermittelt.

Replaced by Article 34 Amended

Method and apparatus for mutual authentication of components in a network using the challenge-response method

The invention relates to a method and an apparatus for mutual authentication of components in a network using the challenge-response method, as claimed in the preamble of claim 1. In particular, the invention relates to mutual authentication of a terminal, preferably a mobile station, with the network, and vice versa. The following text uses the term "mobile station"; this should not be regarded as a limitation. This term is intended to cover all possible terminals, including stationary terminals, such as individual users of a computer in a wire-based system.

Authentication is used to check the authenticity of the component to be authenticated.

The prior art is the so-called challenge-response method: in this method, a random number (challenge) is sent by the authenticating component (N = network) to the component (M = mobile station) to be authenticated and is converted into a response using an algorithm (A) and a secret key K which is known to both components. The expected response is calculated in the network N using the same key K and the same algorithm A; a match between the response sent back by M and the response calculated in N proves the authenticity of M.

Mutual authentication is achieved according to the prior art by the above sequence being carried out with the opposite role distribution.

Accordingly, in the known challenge-response method, the fixed network passes a challenge to the mobile station M, and the

Patent claims

1. A method for mutual authentication of components in a network using the challenge-response method, in which, in order to authenticate a terminal, in particular a mobile station, with the network, the network (N) uses a request to request from an authentication center (AUC) at least one data pair (Challenge 1, Response 1), and passes the data set (Challenge 1) to the terminal (M) which uses an internally stored key (Ki) likewise to calculate from this a Response 1 and sends this to the network (N), in which case, furthermore, the network (N) is authenticated with the terminal (M) wherein, instead of the request for a data pair (Challenge 1/Response 1) from the network N to the AUC, a triplet data set (Challenge 1/Response 1/Response 2) is now requested by the network from the AUC, and wherein the Challenge 2 sent from the terminal (M) to the network (N) is identical to the Response 1, and wherein the network (N) then sends a Response 2 to the terminal (M).

2. The method as claimed in claim 1, wherein the transmission of Challenge 2 is dispensed with and the network interprets the Response 1, which is sent back from the terminal (M), as the Challenge 2.

3. The method as claimed in claim 1 or 2, wherein the data pair (Challenge 1/Response 2) is transmitted from the network (N) to the terminal (M) simultaneously in the form of a single data set (Fig. 3).

4. The method as claimed in claim 1 or 2, wherein the data pair (Challenge 1/Response 2) is transmitted from the network (N) to the terminal (M) simultaneously in the form of a single data set (Fig. 3).

5. The method as claimed in one of claims 2, 3 or 4, wherein the network requests data sets from the authentication center (AUC) in the form of triplet data sets (Challenge 1/Response 1/Response 2).

6. The method as claimed in claim 5, wherein a plurality of triplet data sets are supplied from the AUC as a stockpile, in order to reduce the request frequency.

7. The method as claimed in claim 4 or 5, wherein, in order to use the Response 1 of the terminal (M) as the

Challenge in order to authenticate the network with the terminal (M), the shorter length of the Response 1 is filled out to make up the greater length of the Challenge.

8. The method as claimed in claim 7, wherein the filling-out process is carried out on a subscriber-specific basis, and wherein the

complete length of the Response 1 is shortened before transmission to the other station.

9. The method as claimed in claim 8, wherein the Response 1 is filled out with defined bits from the secret key Ki to make up the length of the Challenge 2.

10. The method as claimed in claim 8, wherein the challenge corresponds to the original Response 1 before it was shortened.

11. Use of the method as claimed in one of claims 1-10, wherein the network is a GSM network.

12. Use of the method as claimed in one of claims 1-10, wherein the network is a wire-based network.

13. The use as claimed in claim 12, wherein the individual, mutually authenticating components in a wire-based network are different monitoring units of computers which authenticate themselves with a central computer, and vice versa.

14. An apparatus for mutual authentication of components in a network as claimed in one of claims 1-13, wherein the AUC calculates the triplet data sets requested by the

network and transmits these to the network off-line and independently of time, on request by the network, but in any case before the data interchange between the network and the terminal.

10
T

R14

Translation

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference 12343.3-D1461	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/DE98/01922	International filing date (*day/month/year*) 10 July 1998 (10.07.1998)	Priority date (*day/month/year*) 10 July 1997 (10.07.1997)
International Patent Classification (IPC) or national classification and IPC H04L 9/32		
Applicant DETEMOBIL DEUTSCHE TELEKOM MOBILNET GMBH		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 5 sheets, including this cover sheet.

   ☒ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 4 sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☐ Priority
   - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
   - VI ☐ Certain documents cited
   - VII ☐ Certain defects in the international application
   - VIII ☐ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
09 February 1999 (09.02.1999)	09 September 1999 (09.09.1999)
Name and mailing address of the IPEA/EP European Patent Office D-80298 Munich, Germany Facsimile No. 49-89-2399-4465	Authorized officer Telephone No. 49-89-2399-0

Form PCT/IPEA/409 (cover sheet) (January 1994)

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/DE98/01922

I. Basis of the report

1. This report has been drawn on the basis of (*Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

☐ the international application as originally filed.

☒ the description, pages 2-10, as originally filed,
pages _____, filed with the demand,
pages 1, filed with the letter of 19 August 1999 (19.08.1999),
pages _____, filed with the letter of _____.

☒ the claims, Nos. _____, as originally filed,
Nos. _____, as amended under Article 19,
Nos. _____, filed with the demand,
Nos. 1-14, filed with the letter of 19 August 1999 (19.08.1999),
Nos. _____, filed with the letter of _____.

☒ the drawings, sheets/fig 1/1, as originally filed,
sheets/fig _____, filed with the demand,
sheets/fig _____, filed with the letter of _____,
sheets/fig _____, filed with the letter of _____.

2. The amendments have resulted in the cancellation of:

☐ the description, pages _____
☐ the claims, Nos. _____
☐ the drawings, sheets/fig _____

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

4. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-14	YES
	Claims		NO
Inventive step (IS)	Claims	1-14	YES
	Claims		NO
Industrial applicability (IA)	Claims	1-14	YES
	Claims		NO

2. Citations and explanations

1. The invention pertains to a process (Claim 1) and a device (Claim 14) for mutual authentication of components in a network.

2. The "challenge-response" process (see D1) wherein a random number ("challenge") is sent by the authenticating component (the network) to the component to be authenticated (a mobile station), said number being converted into a response using an algorithm and a secret key, represents the prior art. The anticipated response is calculated in the network using the same key and the same algorithm and transmitted as a data pair to the network following a challenge. Agreement validates the mobile station. To authenticate the network, the process is repeated in reverse.

   Further, the algorithm and the key are administered in an authentication centre, challenge/response pairs being transmitted to the network in advance for the purposes of authentication.

3. However, central administration of network authentication means that the response to the

challenge sent by the mobile station can be calculated in the authentication centre only, leading to delay.

4. This problem is solved as per the invention by simultaneously using the response sent by the mobile station to the network as a random number ("challenge 2") for the network. Since the network already knows this number, the response based on it ("response 2") may be requested in advance from the authentication centre, thereby considerably accelerating the authentication process.

Since neither the problem nor the solution is disclosed by or may be obviously deduced from D1, Claim 1 meets the requirements of PCT Article 33 (1)-(3).

5. Claims 2-14 are dependent on Claim 1 and therefore likewise meet the requirements of PCT Article 33 (1)-(3).

I. Basis of the report

1. This report has been drawn up on the basis of the following elements *(the replacement sheets received by the receiving office in response to an invitation according to Article 14 are considered in the present report as "originally filed" and are not annexed to the report as they contain no amendments.):*

Description, pages:

2-10	as originally filed			
1	received on	21/08/1999	with the letter of	19/08/1999

Claims, No.:

1-14	received on	21/08/1999	with the letter of	19/08/1999

Drawings, sheets:

1/1	as originally filed

2. The amendments have resulted in the cancellation of:

☐ the description, pages:

☐ the claims, Nos.:

☐ the drawings, sheets:

3. ☐ The present report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated as follows (Rule 70.2(c)):

4. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty	Yes:	Claims	1-14
	No:	Claims	
Inventive Step	Yes:	Claims	1-14
	No:	Claims	
Industrial Applicability	Yes:	Claims	1-14
	No:	Claims	

2. Citations and explanations

See separate sheet

Re Item V

Reasoned statement in accordance with Article 35(2) with regard to novelty, inventive step and commercial applicability; documents and explanations to support this statement

1. The invention relates to a method (claim 1) and an apparatus (claim 14) for mutual authentication of components in a network.

2. The prior art is the so-called "challenge-response method" (see D1), in which a random number ("challenge") is sent by the authenticating component (the network) to the component (a mobile station) to be authenticated, and is converted using an algorithm and a secret key into a response. The expected response is calculated in the network using the same key and the same algorithm, and is transmitted as a data pair to the network on the basis of a request. A match confirms the authenticity of the mobile station. The method is repeated in the opposite direction, in order to authenticate the network.

   It is also known for the algorithm and the key to be controlled in a central authentication centre, with challenge/response pairs being transmitted to the network in advance, for the purpose of authentication.

3. With such central control, a problem arises during authentication of the network in that the response to the challenge sent by the mobile station can be calculated only in the authentication centre, which leads to a delay.

4. According to the invention, this problem is solved in that the response sent by the mobile station to the network is also used as a random number "(Challenge 2") for the network; since the network already knows this number, the response ("Response 2") based on it may be requested even

in advance by the authentication centre. The authentication process is thus considerably speeded up.

Since neither the problem nor the solution from D1 is known or can be derived in an obvious manner, claim 1 satisfies the requirements of Article 33(1)-(3) PCT.

5. Claims 2-14 are dependent on Claim 1, and thus likewise satisfy the requirements of Article 33(1)-(3) PCT.

PATENT COOPERATION TREATY

From the
INTERNATIONAL PRELIMINARY EXAMINING AUTHORITY

To:
RIEBLING, Peter
Postfach 3160
D-88113 Lindau
GERMANY

PCT

NOTIFICATION OF TRANSMITTAL OF INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Rule 71.1)

	Date of mailing *(day/month/year)* 09.09.99
Applicant's or agent's file reference 12343.3-D1461	IMPORTANT NOTIFICATION

International application No. PCT/DE98/01922	International filing date *(day/month/year)* 10/07/1998	Priority date *(day/month/year)* 10/07/1997

Applicant
DETEMOBIL DEUTSCHE TELEKOM MOBILNET GMBH et al.

1. The applicant is hereby notified that this International Preliminary Examining Authority transmits herewith the international preliminary examination report and its annexes, if any, established on the international application.

2. A copy of the report and its annexes, if any, is being transmitted to the International Bureau for communication to all the elected Offices.

3. Where required by any of the elected Offices, the International Bureau will prepare an English translation of the report (but not of any annexes) and will transmit such translation to those Offices.

4. REMINDER

   The applicant must enter the national phase before each elected Office by performing certain acts (filing translations and paying national fees) within 30 months from the priority date (or later in some Offices) (Article 39(1)) (see also the reminder sent by the International Bureau with Form PCT/IB/301).

   Where a translation of the international application must be furnished to an elected Office, that translation must also contain a translation of any annexes to the International preliminary examination report. It is the applicant's responsibility to prepare and furnish such translation directly to each elected Office concerned.

   For further details on the applicable time limits and requirements of the elected Offices, see Volume II of the PCT Applicant's Guide.

Name and mailing address of the IPEA/	Authorized officer:
European Patent Office D-80298 Munich Tel. (+ 49-89) 2399-0, Tx: 523656 epmu d Fax: (+ 49-89) 2399-4465	Bapisch, A Telephone No. +49 99 2399-2262

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

Absender: MIT DER INTERNATIONALEN VORLÄUFIGEN PRÜFUNG BEAUFTRAGTE BEHÖRDE

An:

RIEBLING, Peter
Postfach 3160
D-88113 Lindau
ALLEMAGNE

Vorlage | Ablage | D1461
Haupttermin
Eing.: 10. SEP. 1999
PA. Dr. Peter Riebling
Bearb.: | Vorgelegt:

PCT

MITTEILUNG ÜBER DIE ÜBERSENDUNG DES INTERNATIONALEN VORLÄUFIGEN PRÜFUNGSBERICHTS

(Regel 71.1 PCT)

Absendedatum *(Tag/Monat/Jahr)* 09.09.99	
Aktenzeichen des Anmelders oder Anwalts: 12343.3-D1461	WICHTIGE MITTEILUNG

Internationales Aktenzeichen	Internationales Anmeldedatum *(Tag/Monat/Jahr)*	Prioritätsdatum *(Tag/Monat/Jahr)*
PCT/DE98/01922	10/07/1998	10/07/1997

Anmelder: DETEMOBIL DEUTSCHE TELEKOM MOBILNET GMBH et al.

1. Dem Anmelder wird mitgeteilt, daß ihm die mit der internationalen vorläufigen Prüfung beauftragte Behörde hiermit den zu der internationalen Anmeldung erstellten internationalen vorläufigen Prüfungsbericht, gegebenenfalls mit den dazugehörigen Anlagen, übermittelt.

2. Eine Kopie des Berichts wird - gegebenenfalls mit den dazugehörigen Anlagen - dem Internationalen Büro zur Weiterleitung an alle ausgewählten Ämter übermittelt.

3. Auf Wunsch eines ausgewählten Amts wird das Internationale Büro eine Übersetzung des Berichts (jedoch nicht der Anlagen) ins Englische anfertigen und diesem Amt übermitteln.

4. **ERINNERUNG**

   Zum Eintritt in die nationale Phase hat der Anmelder vor jedem ausgewählten Amt innerhalb von 30 Monaten ab dem Prioritätsdatum (oder in manchen Ämtern noch später) bestimmte Handlungen (Einreichung von Übersetzungen und Entrichtung nationaler Gebühren) vorzunehmen (Artikel 39 (1)) (siehe auch die durch das Internationale Büro im Formblatt PCT/IB/301 übermittelte Information).

   Ist einem ausgewählten Amt eine Übersetzung der internationalen Anmeldung zu übermitteln, so muß diese Übersetzung auch Übersetzungen aller Anlagen zum internationalen vorläufigen Prüfungsbericht enthalten. Es ist Aufgabe des Anmelders, solche Übersetzungen anzufertigen und den betroffenen ausgewählten Ämtern direkt zuzuleiten.

   Weitere Einzelheiten zu den maßgebenden Fristen und Erfordernissen der ausgewählten Ämter sind Band II des PCT-Leitfadens für Anmelder zu entnehmen.

Name und Postanschrift der mit der internationalen Prüfung beauftragten Behörde
Europäisches Patentamt
D-80298 München
Tel. +49 89 2399 - 0 Tx: 523656 epmu d
Fax: +49 89 2399 - 4465

Bevollmächtigter Bediensteter
Bapisch, A
Tel. +49 89 2399-2262

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT
AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER RECHERCHENBERICHT

(Artikel 18 sowie Regeln 43 und 44 PCT)

Aktenzeichen des Anmelders oder Anwalts T97014 PCT	**WEITERES VORGEHEN**	siehe Mitteilung über die Übermittlung des internationalen Recherchenberichts (Formblatt PCT/ISA/220) sowie, soweit zutreffend, nachstehender Punkt 5
Internationales Aktenzeichen PCT/DE 98/ 01922	Internationales Anmeldedatum *(Tag/Monat/Jahr)* 10/07/1998	(Frühestes) Prioritätsdatum *(Tag/Monat/Jahr)* 10/07/1997
Anmelder DETEMOBIL DEUTSCHE TELEKOM MOBILNET GMBH et al.		

Dieser internationale Recherchenbericht wurde von der Internationalen Recherchenbehörde erstellt und wird dem Anmelder gemäß Artikel 18 übermittelt. Eine Kopie wird dem Internationalen Büro übermittelt.

Dieser internationale Recherchenbericht umfaßt insgesamt 2 Blätter.

[X] Darüber hinaus liegt ihm jeweils eine Kopie der in diesem Bericht genannten Unterlagen zum Stand der Technik bei.

1. [ ] **Bestimmte Ansprüche haben sich als nichtrecherchierbar erwiesen** (siehe Feld I).

2. [ ] **Mangelnde Einheitlichkeit der Erfindung** (siehe Feld II).

3. [ ] In der internationalen Anmeldung ist **ein Protokoll einer Nucleotid- und/oder Aminosäuresequenz** offenbart; die internationale Recherche wurde auf der Grundlage des Sequenzprotokolls durchgeführt,
   - [ ] das zusammen mit der internationalen Anmeldung eingereicht wurde.
   - [ ] das vom Anmelder getrennt von der internationalen Anmeldung vorgelegt wurde,
     - [ ] dem jedoch keine Erklärung beigefügt war, daß der Inhalt des Protokolls nicht über den Offenbarungsgehalt der internationalen Anmeldung in der eingereichten Fassung hinausgeht.
   - [ ] das von der Internationalen Recherchenbehörde in die ordnungsgemäße Form übertragen wurde.

4. Hinsichtlich der **Bezeichnung der Erfindung**
   - [X] wird der vom Anmelder eingereichte Wortlaut genehmigt.
   - [ ] wurde der Wortlaut von der Behörde wie folgt festgesetzt.

5. Hinsichtlich der **Zusammenfassung**
   - [X] wird der vom Anmelder eingereichte Wortlaut genehmigt.
   - [ ] wurde der Wortlaut nach Regel 38.2b) in der Feld III angegebenen Fassung von dieser Behörde festgesetzt. Der Anmelder kann der Internationalen Recherchenbehörde innerhalb eines Monats nach dem Datum der Absendung dieses internationalen Recherchenberichts eine Stellungnahme vorlegen.

6. Folgende Abbildung der **Zeichnungen** ist mit der Zusammenfassung zu veröffentlichen:
   Abb. Nr. 2
   - [ ] wie vom Anmelder vorgeschlagen
   - [X] weil der Anmelder selbst keine Abbildung vorgeschlagen hat.
   - [ ] weil diese Abbildung die Erfindung besser kennzeichnet.
   - [ ] keine der Abb.

PCT

WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 6 : H04Q 7/00 — A2

(11) Internationale Veröffentlichungsnummer: WO 99/03285

(43) Internationales Veröffentlichungsdatum: 21. Januar 1999 (21.01.99)

(21) Internationales Aktenzeichen: PCT/DE98/01922

(22) Internationales Anmeldedatum: 10. Juli 1998 (10.07.98)

(30) Prioritätsdaten:
197 29 611.4 10. Juli 1997 (10.07.97) DE
197 30 301.3 15. Juli 1997 (15.07.97) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: DE-TEMOBIL DEUTSCHE TELEKOM MOBILNET GMBH [DE/DE]; Landgrabenweg 151, D-53227 Bonn (DE).

(71) Anmelder *(nur für US)*: PERNICE, Edith (Erbin des verstorbenen Erfinders) [DE/DE]; Schillerstrasse 11, D-64846 Groß-Zimmern (DE).

(72) Erfinder: PERNICE, Frieder (verstorben).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: MARINGER, Günter [DE/DE]; Troschelstrasse 8, D-53115 Bonn (DE). MOHRS, Walter [DE/DE]; Rosenhain 3, D-53123 Bonn (DE).

(74) Anwalt: RIEBLING, Peter; Postfach 3160, D-88113 Lindau (DE).

(81) Bestimmungsstaaten: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CZ, DK, EE, ES, FI, GB, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO Patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht
Ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts.

(54) Title: METHOD AND DEVICE FOR THE MUTUAL AUTHENTICATION OF COMPONENTS IN A NETWORK USING THE CHALLENGE-RESPONSE METHOD

(54) Bezeichnung: VERFAHREN UND VORRICHTUNG ZUR GEGENSEITIGEN AUTHENTISIERUNG VON KOMPONENTEN IN EINEM NETZ MIT DEM CHALLENGE-RESPONSE-VERFAHREN

(57) Abstract

The invention relates to a method for the mutual authentication of components in a network by means of the challenge-response method, according to which the network (N) requests a set of three data values (challenge 1/ response 1/ response 2) from an authentication centre (AUC) and transmits at least one set of data values (challenge 1) to the mobile station (M) which on the basis of an internally stored key (Ki) calculates a response 1 from this set of data values and transmit it to the network (N). To authenticate the network (N) in relation to the mobile station (M) the invention provides for the response 1 sent back to the network (N) to be interpreted simultaneously by said network (N) as challenge 2 and for said network (N) immediately to transmit a response 2 to the mobile station (M). This improves and accelerates data traffic between the mobile station and the network because there is no transmission of challenge 2 between the mobile station and the network. Data traffic between the network and the AUC is also improved because the data pairs challenge 2 and response 2 no longer have to be calculated separately in the AUC and transmitted to the network.

(57) Zusammenfassung

Es wird ein Verfahren zur gegenseitigen Authentisierung von Komponenten in einem Netz nach dem Challenge-Response-Verfahren beschrieben, bei dem das Netz (N) von einem Authentisierungszentrum (AUC) einen Dreier-Datensatz (Challenge 1/Response 1/Response 2) anfordert und mindestens einen Datensatz (Challenge 1) an die Mobilstation weiterleitet, welche aufgrund eines intern gespeicherten Schlüssels (Ki) hieraus eine Response 1 berechnet und an das Netz (N) absendet. Zur Authentisierung des Netzes (N) gegenüber der Mobilstation (M) ist vorgesehen, daß die an das Netz (N) zurückgesandte Response 1 gleichzeitig vom Netz (N) als Challenge 2 interpretiert wird, und daß das Netz (N) hierauf sofort eine Response 2 an die Mobilstation (M) sendet. Hierdurch wird der Datenverkehr zwischen der Mobilstation und dem Netz verbessert und beschleunigt, denn es wird auf die Übertragung der Challenge 2 zwischen Mobilstation und Netz verzichtet. Ebenso wird der Datenverkehr zwischen dem Netz und dem AUC verbessert, denn die Datenpaare Challenge 2 und Response 2 müssen nicht mehr im AUC gesondert berechnet und an das Netz weitergeleitet werden.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	ES	Spanien	LS	Lesotho	SI	Slowenien
AM	Armenien	FI	Finnland	LT	Litauen	SK	Slowakei
AT	Österreich	FR	Frankreich	LU	Luxemburg	SN	Senegal
AU	Australien	GA	Gabun	LV	Lettland	SZ	Swasiland
AZ	Aserbaidschan	GB	Vereinigtes Königreich	MC	Monaco	TD	Tschad
BA	Bosnien-Herzegowina	GE	Georgien	MD	Republik Moldau	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagaskar	TJ	Tadschikistan
BE	Belgien	GN	Guinea	MK	Die ehemalige jugoslawische Republik Mazedonien	TM	Turkmenistan
BF	Burkina Faso	GR	Griechenland			TR	Türkei
BG	Bulgarien	HU	Ungarn	ML	Mali	TT	Trinidad und Tobago
BJ	Benin	IE	Irland	MN	Mongolei	UA	Ukraine
BR	Brasilien	IL	Israel	MR	Mauretanien	UG	Uganda
BY	Belarus	IS	Island	MW	Malawi	US	Vereinigte Staaten von Amerika
CA	Kanada	IT	Italien	MX	Mexiko		
CF	Zentralafrikanische Republik	JP	Japan	NE	Niger	UZ	Usbekistan
CG	Kongo	KE	Kenia	NL	Niederlande	VN	Vietnam
CH	Schweiz	KG	Kirghistan	NO	Norwegen	YU	Jugoslawien
CI	Côte d'Ivoire	KP	Demokratische Volksrepublik Korea	NZ	Neuseeland	ZW	Zimbabwe
CM	Kamerun			PL	Polen		
CN	China	KR	Republik Korea	PT	Portugal		
CU	Kuba	KZ	Kasachstan	RO	Rumänien		
CZ	Tschechische Republik	LC	St. Lucia	RU	Russische Föderation		
DE	Deutschland	LI	Liechtenstein	SD	Sudan		
DK	Dänemark	LK	Sri Lanka	SE	Schweden		
EE	Estland	LR	Liberia	SG	Singapur		

514 Rec'd PCT/PTO 09/462616 10 JAN 2000

WO 99/03285 1/PRTS PCT/DE98/01922

Verfahren und Vorrichtung zur gegenseitigen Authentisierung von Komponenten in einem Netz mit dem Challenge-Response-Verfahren.

Die Erfindung betrifft ein Verfahren und eine Vorrichtung zur gegenseitigen Authentisierung von Komponenten in einem Netz mit dem Challenge-Response-Verfahren nach dem Oberbegriff des Anspruches 1. Insbesondere betrifft die Erfindung die gegenseitige Authentisierung eines Endgeräts, bevorzugt einer Mobilstation gegenüber dem Netz und umgekehrt. Im folgenden wird der Begriff „Mobilstation" verwendet; dies ist nicht einschränkend zu verstehen. Hierunter sollen alle möglichen Endgeräte fallen, auch stationäre, wie z.B. einzelne Nutzer eines Computers in einem drahtgebundenen System.

Authentisieren dient zur Überprüfung der Echtheit der zu authentisierenden Komponente.
Stand der Technik ist das sogenannte Challenge-Response-Verfahren: Bei diesem wird von der authentisierenden Komponente (N = Netz) eine Zufallszahl (Challenge) an die zu authentisierende Komponente (M = Mobilstation) gesandt, die mit Hilfe eines Algorithmus (A) und eines geheimen, beiden Komponenten bekannten Schlüssels K in eine Antwort (Response) umgerechnet wird. Im Netz N wird mit gleichem Schlüssel K und dem gleichen Algorithmus A die erwartete Response errechnet; eine Übereinstimmung der von M zurückgesendeten mit der bei N errechneten Response beweist die Echtheit von M.
Eine gegenseitige Authentisierung wird nach Stand der Technik dadurch erreicht, daß der obige Ablauf mit umgekehrter Rollenverteilung stattfindet.

Bei dem bekannten Challenge-Response-Verfahren gibt demnach das Festnetz eine Challenge an die Mobilstation M und die

Mobilstation M antwortet mit einer Response, die aus einem Rechenverfahren errechnet wurde, das in der Mobilstation implementiert ist und zu der ein geheimer Schlüssel K gehört. Dieser Schlüssel K ist einmalig. D. h. nur diese Mobilstation kann so antworten, wie es von ihr erwartet wird, sofern sie "echt" = authentisiert ist. Eine andere Mobilstation (M) kann diesen Schlüssel nicht simulieren.

Nachteil des bisherigen Verfahrens ist, daß das gesamte Authentisierungsverfahren nur und ausschließlich in der AUC (Authentisierungszentrale), das heißt praktisch in der Rechenzentrale, verifiziert werden kann.

Aus Sicherheitsgründen hat es sich nämlich in Systemarchitekturen als vorteilhaft erwiesen, A und K an zentraler Stelle (im Authentication Center = AUC) zu verwalten, wobei der authentisierenden (die Echtheitsprüfung durchführenden) Stelle N zum Zwecke der Authentisierung nur Challenge/Response-Paare im voraus (ggf. mehrere auf Vorrat) übertragen werden.

Die vom AUC in das Netz (auf Anforderung des Netzes in Form eines sogenannten „Duplet Request") übergebenen Challenge/Response-Paare werden also in großem Umfang bereits schon „auf Vorrat" errechnet und wenn während des Authentisierungsvorgangs die Antwort (Response) von der Mobilstation M kommt, werden beide Anworten verglichen. Bei Übereinstimmung ist damit das Authentisierungsverfahren der Mobilstation M gegenüber dem Netz N erfolgreich beendet.

Bei den bekannten Verfahren des Standes der Technik ist demnach vorgesehen, daß sich die Mobilstationen gegenüber dem Netz authentisieren. Es besteht damit die Gefahr, daß von Unbefugten

das Netz simuliert wird und daß damit die betreffende Mobilstation M an das simulierte Netz „angelockt" wird und hierbei der Mobilstation M vorgespiegelt wird, es handele sich hierbei um das „richtige" Netz N. Für diesen unerlaubten Fall würde sich die M gegenüber dem simulierten Netz N authentisieren und damit kann der unbefugte Betreiber des simulierten Netzes nichtöffentliche Daten aus dieser Mobilstation M abrufen.

Als Beispiel sei das GSM-Netz genannt, das bisher nur eine einseitige Authentisierung. vornimmt (M authentisiert sich gegenüber N). Beim ferner bekannten TETRA-Standard, ist eine zweiseitige Authentisierung erlaubt.

Zur besseren Verdeutlichung der später verwendeten Begriffe „Challenge 1, Response 1 und Challenge 2, Resonse 2", wird nachfolgend das Verfahren erläutert:

Die Challenge 1 dient der Authentikation der Mobilstation M gegenüber dem Netz N. Sobald diese Authentikation erfolgreich abgeschlossen wurde, fordert die Mobilstation M eine umgekehrte Authentifizierung, in der Weise, daß jetzt geprüft wird, ob das derzeitige Netz N auch wirklich das befugte Netz ist und nicht ein unerlaubterweise simuliertes Netz. Es soll sich also das Netz N gegenüber der Mobilstation M authentisieren. Die Mobilstation M schickt hierbei eine Challenge 2 zum Netz, dieses leitet die Challenge 2 zum AUC weiter, wo daraus die Response 2 errechnet wird, die wiederum an das Netz N geschickt wird, welches Response 2 an die Mobilstation weiterleitet. Hat die Mobilstation die Übereinstimmung von der selbst berechneten Response 2 und der erhaltenen Response 2 festgestellt, ist damit die Authentifizierung erfolgreich beendet. Dieses Authentifizierungspaar wird als Challenge 2/Response 2 bezeichnet.

Bei gegenseitiger Authentisierung wirkt sich in solchen Systemarchitekturen nachteilig aus, daß die von M gesandte Challenge nicht in N, sondern nur im AUC in die Response umgerechnet werden kann, was unter Umständen zu erheblichen Zeitverzögerungen wegen des Datentransfers N-AUC-N und der online Rechenoperation im AUC führt.

Der Erfindung liegt die Aufgabe zugrunde, das bekannte Verfahren zur Authentifikation von Komponenten in einem Netz, insbesondere in einem GSM-Netz, so zu verbessern, daß dieses Verfahren wesentlich beschleunigt wird.

Zur Lösung der gestellten Aufgabe ist das Verfahren dadurch gekennzeichnet, daß die von der Mobilstation M zurückgesandte Response 1 gleichzeitig von dem Netz N als Challenge 2 verwendet wird, was den Vorteil hat, daß vom AUC gleichzeitig mit den o.g. Challenge/Response-Paaren auch die Response 2 (als Antwort auf Challenge 2) errechnet und übermittelt wird. Dadurch entfällt die Zeitverzögerung, die auftreten würde, wenn N sich Response 2 erst nach Eintreffen von Challenge 2 beim AUC besorgen müßte.

Damit ist vorgesehen, daß die Mobilstation zur Echtheitserkennung des Netzes N nicht mehr eine Challenge 2 intern erzeugt und an das Netz schickt, sondern daß durch Gleichsetzen der Response 1 mit der Challenge 2 schon gegenseitige Übereinstimmung in M und N über die erwartete Challenge 2 existiert. Das Netz kann somit schon eine Response 2 erzeugen und an die Mobilstation schicken, welche diese Response 2 mit dem bei sich errechneten Wert vergleicht und bei Übereinstimmung das Netz als „echt" anerkennt.

Wichtig hierbei ist also , daß man die von der Mobilstation an das Netz abgeschickte Response 1 gleichzeitig als Challenge 2 dieser Mobilstation benutzt, welche diese aber nicht mehr in das Netz schickt, um auf die Response 2 des Netzes wartet. Die Challenge 2 der Mobilstation kennt das Netz nämlich schon vorher, weil die Response 2 intern bereits schon berechnet wurde. Damit kann das Netz bereits auch schon die Response 2 errechnen.

Erfindungsgemäß laufen die wechselseitige Authentifikation von Mobilstation zum Netz und danachfolgend die Authentifikation von Netz zur Mobilstation nun nicht mehr mit relativ hohem Zeitbedarf zeitlich aufeinanderfolgend ab, sondern die beiden Echtheitsprüfungen werden nun zeitlich miteinander verzahnt.

Es wird damit eine vollständige Datenübertragung einer Prüfzahl (Challenge 2) vermieden, denn erfindungsgemäß kann die Challenge 2 eingespart werden und muß nicht mehr übertragen werden. Die separate Übertragung der Response 2 vom Netz wird dadurch eingespart, als das Netz gleich bei Absendung von Challenge 1 auch bereits schon die Response 2 zur Mobilstation schickt. Begründet wird dies damit, daß das Netz schon vorher weiß, was die Challenge 2 der Mobilstation sein wird, also kann das Netz auch sofort die Response 2 zur Mobilstation schicken. In einer einzigen Datenübertragung überträgt das Netz also die Datenpaarung Challenge 1 / Response 2 zur Mobilstation. Damit wird erreicht, daß die Mobilstation die Echtheit von N bereits erkannt hat, bevor sich M gegenüber N authentisiert hat.

Hierbei gibt es zwei verschiedene Ausführungen :

In einer ersten Ausführungsform übermittelt das Netz an die Mobilstation die Challenge 1. Die Mobilstation M antwortet mit Response 1. Nachdem dem Netz vom AUC vorher aber bereits eine Vielzahl von Dreier-Datenpaketen (Triplet= Challenge 1/ Response 1 / Response 2) übermittelt wurden, kennt das Netz N auch die Response 1 der Mobilstation M im voraus. Mit Kenntnis von Response 1 ist ihm aber auch die Challenge 2 bekannt. Die Mobilstation sendet nun nicht mehr die Challenge 2 zum Netz, sondern das Netz antwortet auf die Response 1 von M mit der Response 2. Diese Kenntnis ist jedoch nur dem „echten" Netz zu eigen; ein simuliertes, unerlaubtes Netz hat diese Kenntnis nicht; damit hat sich das Netz N gegenüber der Mobilstation durch die Übertragung eines einzigen Datenpaktes (Challenge 1 / Response 2) authentisiert und erspart sich die Übertragung des zweiten Datenpaketes (Challenge 2).

Hierbei ist vorteilhaft, daß die Response 2 eine Funktion von Response 1 ist. Das heißt, bei Kenntnis des Funktionszusammenhangs kann aus der Response 1 = Challenge 2 die Response 2 berechnet werden. Nach dem Stand der Technik war die Response 2 eine Funktion von Challenge 2. Erfindungsgemäß muß Challenge 2 nicht mehr übertragen werden, da Challenge 2 = Response 1 eine Funktion von Challenge 1 ist.

Letztendlich gilt durch die Gleichsetzung von Response 1 und Challenge 2, daß Response 2 auch eine Funktion von Challenge 1 ist.

In der ersten Ausgestaltung werden demgemäß Challenge 1 und Response 2 zeitlich hintereinander folgend an die Mobilstation M geschickt.

In einer zweiten Ausgestaltung ist es vorgesehen, daß Challenge 1 und Response 2 als ein Datenpaket zusammen an die Mobilstation M geschickt werden.
Hierauf antwortet die Mobilstation mit Response 1 und jetzt vergleicht das Netz Response 1 mit dem erwarteten Wert von Response 1 und die Mobilstation vergleicht Response 2 mit dem intern errechneten Wert von Response 2.

In bekannten Systemen (z..B. im GSM-Netz) ist die Länge der Response (32 bit) kürzer als die Zufallszahl Challenge (128 bit). Um die Response gleichzeitig als Challenge zur Authentisierung von N gegenüber M mit dem gleichen Algorithmus A benutzen zu können, ist es notwendig, die Länge von Response 1 auf die von Algorithmus A erwartete Länge von 128 bit zu erhöhen.
Dies könnte durch vierfache Verkettung von Response 1 (4 x 32 bit = 128 bit) oder durch vorher definiertes (teilnehmerindividuelles oder teilnehmerunabhängiges) Auffüllen auf 128 bit erreicht werden.

Vorschläge für das teilnehmerindividuelle Auffüllen sind:

1 . Hernahme des kompletten Rechenergebnisses von Response 1 , bevor es zur Übertragung zur Gegenstelle auf 32 bit verkürzt wurde

2.. Auffüllen mit definierten Bits aus dem in M und AUC bekannten K_i.

Der Vorteil beider Ausführungsformen gegenüber dem Stand der Technik liegt also darin, daß der Datenverkehr zwischen dem Netz und der Mobilstation einerseits und auch der Datenverkehr zwischen dem Netz und der AUC vereinfacht und damit beschleunigt wird. Nach dem Stand der Technik müssen vier Telegramme zwischen Netz und Mobilstation M hin und

hergeschickt werden, nämlich Challenge 1, Response 1, Challenge 2 und Response 2.
Außerdem muß das Netz die Challenge 2 erst an das AUC übermitteln und dieses muß die Response 2 errechnen und an das Netz übergeben, was mit weiterem Zeitverlust verbunden ist.

Erfindungsgemäß wird eine zeitaufwendige Online-Abfrage vom Netz an die AUC vermieden. Dies erfolgt dadurch, daß bereits schon vor dem eigentliche Datenverkehr zur Authentifizierung zwischen Netz und Mobilstation die von der AUC hierfür benötigten Datenpakete abgerufen und beim Netz zur späteren Verwendung zwischengespeichert werden.

Derartige Datenpakte (Triplets) können schon in großem zeitlichen Vorlauf (z. B. Stunden oder Tage vorher) vom Netz vom AUC abgerufen werden. Allen beiden Ausführungen ist hierbei gemeinsam, daß man die Response 1 als Challenge 2 benutzt und damit auf die eigentliche Übermittlung von Challenge 2 verzichten kann.

Mehrere bevorzugte Ausführungsbeispiele werden nun anhand der Zeichnungen näher beschrieben. Hierbei gehen aus der Zeichnung und ihrer Beschreibung weitere Merkmale der Erfindung hervor.
Es zeigen :
Fig. 1 : Schematisiert ein Authentifizierungsverfahren nach dem Stand der Technik
Fig. 2 : Eine erste Ausführungsform der Authentifizierung nach der Erfindung
Fig. 3 : Eine zweite Ausführungsform der Authentifizierung nach der Erfindung

In der Ausführung nach Fig. 1 fordert zunächst das Netz N Datensätze als Zweier-Pakete (Duplet-Request) von der AUC an.

Diese Zweier-Pakete enthalten die Datensätze für Challenge 1/Response 1. Sobald sich nun eine Mobilstation M gegenüber dem Netz N authentifizieren soll, sendet N zunächst den Datensatz Challenge 1 an M, welche mit Response 1 antwortet. Falls N eine Übereinstimmung beider Datensätze feststellt, wurde damit die „Echtheit" von M gegenüber N erwiesen. Umgekehrt fordert nun M die Echtheitsprüfung von N dadurch, daß M an N eine Challenge 2 sendet, welche N an AUC weiterleitet, wo daraus die geforderte Response 2 berechnet wird, die AUC an N weitergibt, die dieses wiederum an M absendet. M vergleicht nun die intern berechnete und die von N erhaltene Response 2 und erkennt bei Übereinstimmung beider die Echtheit von N an.

Wie bereits schon eingangs darauf hingewiesen, wird durch diesen vielfältigen Datenaustausch der Verkehr zwischen M und N einerseits und N und AUC andererseits stark belastet und ist daher mit Zeitverzögerungen behaftet.
Hier greift das neue Verfahren in seiner ersten Ausführung gemäß Fig. 2 ein, wo vorgesehen ist, daß N von AUC sogenannte Dreier-Datensätze (Triplets) in Form von Challenge 1/Response 1/Response 2 fordert. Hierbei ist der Datensatz Response 2 eine definierte Funktion des Datensatzes Response 1 und durch einen Algorithmus berechenbar. Derartige Datensätze werden zeitlich längst vor der Abwicklung des Datenverkehrs von N mit M von AUC abgefordert und in Form von Vielfach-Datensätzen in N gespeichert. Hierdurch entfällt die Notwendigkeit des Online-Datenverkehrs zwischen N und AUC, wie es beim Stand der Technik nach Figur 1 notwendig gewesen war.
Zur Authentifizierung von M gegenüber N sendet N an M zunächst die Challenge 1, worauf M mit der Response 1 antwortet. Nachdem N bereits schon den Datensatz Challenge 2 kennt, der beim Stand der Technik von M an N gesendet wird, reicht es aus, wenn N zur Authentifizierung gegenüber M nur noch den Datensatz Response 2

an M sendet. M hat intern den Datensatz Response 2 errechnet und vergleicht diesen mit der von N gesendeten Response 2. Bei Übereinstimmung ist damit die „Echtheit" von N gegenüber M erwiesen.

In der zweiten Ausführungsform des Verfahrens nach Figur 3 ist in Abweichung des Verfahrens nach Figur 2 vorgesehen, daß N sofort und einmalig den Datensatz Challenge 1/Response 2 an M schickt. Sobald M den Datensatz Response 1 zurückschickt ist damit sowohl die Authentifizierung von M gegenüber N als auch umgekehrt von N gegenüber M gelungen.

Patentansprüche

1.Verfahren zur gegenseitigen Authentisierung von Komponenten in einem Netz nach dem Challenge-Response-Verfahren, bei dem zur Authentifizierung eines Endgeräts, insbesondere einer Mobilstation, gegenüber dem Netz das Netz (N) von einem Authentisierungszentrum (AUC) aufgrund einer Anforderung mindestens ein Datenpaar (Challenge 1, Response 1) anfordert und den Datensatz (Challenge 1) an das Endgerät (M) weiterleitet, welche aufgrund eines intern gespeicherten Schlüssels (Ki) hieraus eine Response 1 berechnet und an das Netz (N) absendet, wobei ferner eine Authentisierung des Netzes (N) gegenüber dem Endgerät (M) stattfindet, dadurch gekennzeichnet, daß anstatt der Anforderung von einem Datenpaar (Challenge 1 / Response 1) vom Netz N an das AUC nunmehr ein Dreier-Datensatz (Challenge 1 / Response 1 / Response 2) vom Netz vom AUC angefordert wird und daß die von dem Endgerät (M) an das Netz (N) gesandte Challenge 2 identisch ist mit der Response 1, und daß das Netz (N) hierauf ein Response 2 an das Endgerät (M) sendet.

2.Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß auf die Übertragung von Challenge 2 verzichtet wird und daß das Netz die von dem Endgerät (M) zurückgesandte Response 1 als Challenge 2 interpretiert.

3.Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die Übertragung des Datenpaares (Challenge 1/ Response 2) von dem Netz (N) zu dem Endgerät (M) gleichzeitig in Form eines einzigen Datensatzes erfolgt, (Fig. 3).

4.Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die Übertragung des Datenpaares (Challenge 1/Response 2) von dem Netz (N) zu dem Endgerät(M) gleichzeitig in Form eines einzigen Datensatzes erfolgt, (Fig. 3).

5.Verfahren nach einem der Ansprüche 2, 3 oder 4, dadurch gekennzeichnet, daß das Netz Datensätze vom Authentifizierungszentrum (AUC) in Form von Dreier-Datensätzen (Challenge 1/Response 1/Response 2) anfordert.

6.Verfahren nach Anspruch 5, dadurch gekennzeichnet, daß zur Herabsetzung der Anforderungshäufigkeit mehrere Dreier-Datensätze vom AUC als Vorrat geliefert werden.

7.Verfahren nach Anspruch 4 oder 5, dadurch gekennzeichnet, daß zur Verwendung der Response 1 des Endgeräts (M) als Challenge zwecks Authentifikation des Netzes gegenüber dem Endgerät (M) die kürzere Länge der Response 1 auf die größere Länge der Challenge aufgefüllt wird.

8.Verfahren nach Anspruch 7, dadurch gekennzeichnet, daß das Auffüllen teilnehmer-individuell erfolgt und daß die

vollständige Länge der Response 1 vor der Übertragung auf die Gegenstelle verkürzt wird.

9. Verfahren nach Anspruch 8, dadurch gekennzeichnet, daß die Response 1 mit definierten Bits aus dem geheimen Schlüssel Ki auf die Länge der Challenge 2 aufgefüllt wird.

10. Verfahren nach Anspruch 8, dadurch gekennzeichnet, daß die Challenge der originalen Response 1 vor ihrer Kürzung entspricht.

11. Verwendung des Verfahrens nach einem der Ansprüche 1 - 10, dadurch gekennzeichnet, daß das Netz ein GSM-Netz ist.

12. Verwendung des Verfahrens nach einem der Ansprüche 1 - 10, dadurch gekennzeichnet, daß das Netz ein drahtgebundenes Netz ist.

13. Verwendung nach Anspruch 12, dadurch gekennzeichnet, daß die einzelnen, sich gegenseitig authentisierenden Komponenten in einem drahtgebundenen Netz verschiedene Kontrolleinheiten von Computern sind, welche sich gegenüber einem Zentralcomputer authentifizieren und umgekehrt.

14. Vorrichtung zur gegenseitigen Authentisierung von Komponenten in einem Netzwerk nach einem der Ansprüche 1 - 13, dadurch gekennzeichnet, daß das AUC die vom Netz geforderten Dreier-Datensätze berechnet und auf Anforderung vom Netz diese Off-Line und zeitlich unabhängig, jedoch auf jeden Fall vor dem Datenaustausch zwischen Netz und Endgerät an das Netz übermittelt.

09/462616

WO 99/03285

PCT/DE98/01922

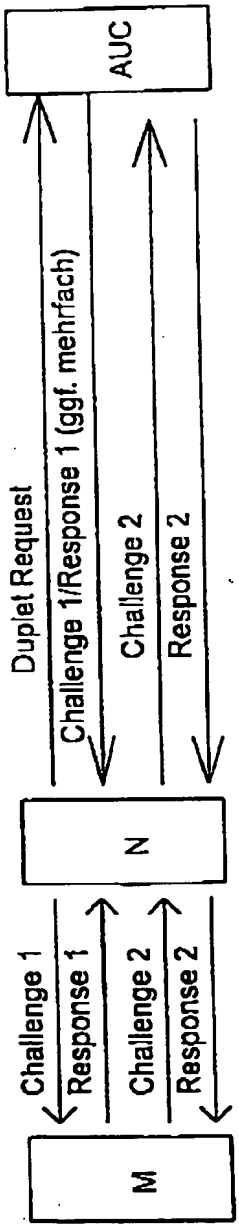


Fig. 1

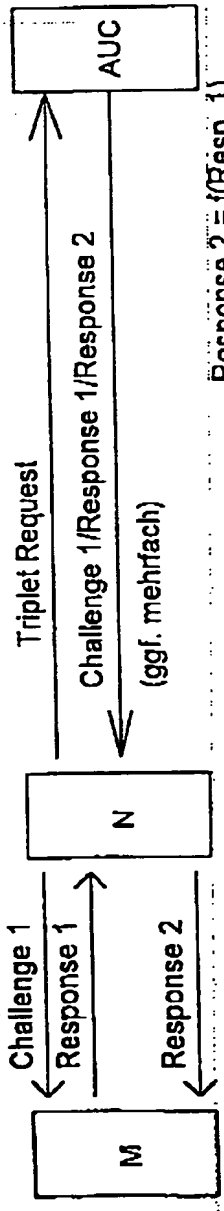


Fig. 2

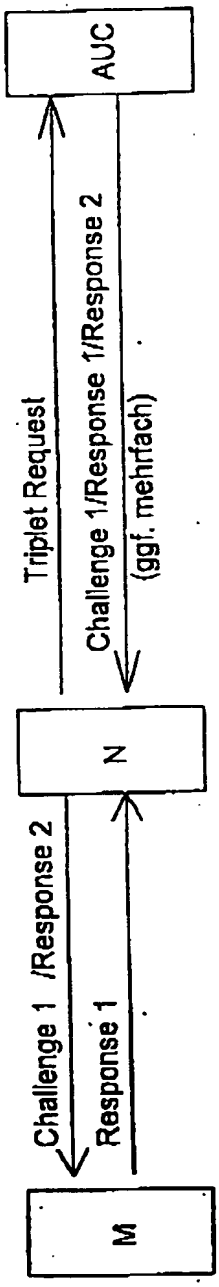


Fig. 3

PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 6: H04L 9/32, H04Q 7/38 — A3

(11) Internationale Veröffentlichungsnummer: WO 99/03285

(43) Internationales Veröffentlichungsdatum: 21. Januar 1999 (21.01.99)

(21) Internationales Aktenzeichen: PCT/DE98/01922

(22) Internationales Anmeldedatum: 10. Juli 1998 (10.07.98)

(30) Prioritätsdaten:
197 29 611.4 10. Juli 1997 (10.07.97) DE
197 30 301.3 15. Juli 1997 (15.07.97) DE

(71) Anmelder (*für alle Bestimmungsstaaten ausser US*): DE-TEMOBIL DEUTSCHE TELEKOM MOBILNET GMBH [DE/DE]; Landgrabenweg 151, D-53227 Bonn (DE).

(71) Anmelder (*nur für US*): PERNICE, Edith (Erbin des verstorbenen Erfinders) [DE/DE]; Schillerstrasse 11, D-64846 Groß-Zimmern (DE).

(72) Erfinder: PERNICE, Frieder (verstorben).

(72) Erfinder; und
(75) Erfinder/Anmelder (*nur für US*): MARINGER, Günter [DE/DE]; Troschelstrasse 8, D-53115 Bonn (DE). MOHRS, Walter [DE/DE]; Rosenhain 3, D-53123 Bonn (DE).

(74) Anwalt: RIEBLING, Peter; Postfach 3160, D-88113 Lindau (DE).

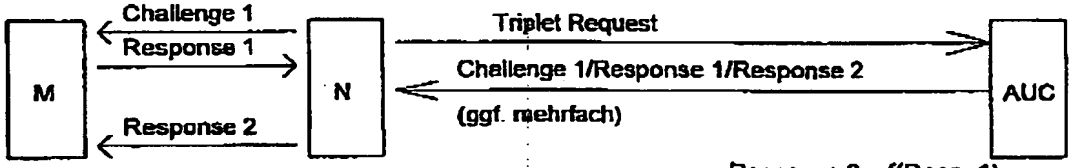
(81) Bestimmungsstaaten: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CZ, DK, EE, ES, FI, GB, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO Patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht
Mit internationalem Recherchenbericht.

(88) Veröffentlichungsdatum des internationalen Recherchenberichts: 1. April 1999 (01.04.99)

(54) Title: METHOD AND DEVICE FOR THE MUTUAL AUTHENTICATION OF COMPONENTS IN A NETWORK USING THE CHALLENGE-RESPONSE METHOD

(54) Bezeichnung: VERFAHREN UND VORRICHTUNG ZUR GEGENSEITIGEN AUTHENTISIERUNG VON KOMPONENTEN IN EINEM NETZ MIT DEM CHALLENGE-RESPONSE-VERFAHREN



(57) Abstract

The invention relates to a method for the mutual authentication of components in a network by means of the challenge-response method, according to which the network (N) requests a set of three data values (challenge 1/ response 1/ response 2) from an authentication centre (AUC) and transmits at least one set of data values (challenge 1) to the mobile station (M) which on the basis of an internally stored key (Ki) calculates a response 1 from this set of data values and transmit it to the network (N). To authenticate the network (N) in relation to the mobile station (M) the invention provides for the response 1 sent back to the network (N) to be interpreted simultaneously by said network (N) as challenge 2 and for said network (N) immediately to transmit a response 2 to the mobile station (M). This improves and accelerates data traffic between the mobile station and the network because there is no transmission of challenge 2 between the mobile station and the network. Data traffic between the network and the AUC is also improved because the data pairs challenge 2 and response 2 no longer have to be calculated separately in the AUC and transmitted to the network.

(57) Zusammenfassung

Es wird ein Verfahren zur gegenseitigen Authentisierung von Komponenten in einem Netz nach dem Challenge-Response-Verfahren beschrieben, bei dem das Netz (N) von einem Authentisierungszentrum (AUC) einen Dreier-Datensatz (Challenge 1/Response 1/Response 2) anfordert und mindestens einen Datensatz (Challenge 1) an die Mobilstation weiterleitet, welche aufgrund eines intern gespeicherten Schlüssels (Ki) hieraus eine Response 1 berechnet und an das Netz (N) absendet. Zur Authentisierung des Netzes (N) gegenüber der Mobilstation (M) ist vorgesehen, daß die an das Netz (N) zurückgesandte Response 1 gleichzeitig vom Netz (N) als Challenge 2 interpretiert wird, und daß das Netz (N) hierauf sofort eine Response 2 an die Mobilstation (M) sendet. Hierdurch wird der Datenverkehr zwischen der Mobilstation und dem Netz verbessert und beschleunigt, denn es wird auf die Übertragung der Challenge 2 zwischen Mobilstation und Netz verzichtet. Ebenso wird der Datenverkehr zwischen dem Netz und dem AUC verbessert, denn die Datenpaare Challenge 2 und Response 2 müssen nicht mehr im AUC gesondert berechnet und an das Netz weitergeleitet werden.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	ES	Spanien	LS	Lesotho	SI	Slowenien
AM	Armenien	FI	Finnland	LT	Litauen	SK	Slowakei
AT	Österreich	FR	Frankreich	LU	Luxemburg	SN	Senegal
AU	Australien	GA	Gabun	LV	Lettland	SZ	Swasiland
AZ	Aserbaidschan	GB	Vereinigtes Königreich	MC	Monaco	TD	Tschad
BA	Bosnien-Herzegowina	GE	Georgien	MD	Republik Moldau	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagaskar	TJ	Tadschikistan
BE	Belgien	GN	Guinea	MK	Die ehemalige jugoslawische Republik Mazedonien	TM	Turkmenistan
BF	Burkina Faso	GR	Griechenland			TR	Türkei
BG	Bulgarien	HU	Ungarn	ML	Mali	TT	Trinidad und Tobago
BJ	Benin	IE	Irland	MN	Mongolei	UA	Ukraine
BR	Brasilien	IL	Israel	MR	Mauretanien	UG	Uganda
BY	Belarus	IS	Island	MW	Malawi	US	Vereinigte Staaten von Amerika
CA	Kanada	IT	Italien	MX	Mexiko		
CF	Zentralafrikanische Republik	JP	Japan	NE	Niger	UZ	Usbekistan
CG	Kongo	KE	Kenia	NL	Niederlande	VN	Vietnam
CH	Schweiz	KG	Kirgisistan	NO	Norwegen	YU	Jugoslawien
CI	Côte d'Ivoire	KP	Demokratische Volksrepublik Korea	NZ	Neuseeland	ZW	Zimbabwe
CM	Kamerun			PL	Polen		
CN	China	KR	Republik Korea	PT	Portugal		
CU	Kuba	KZ	Kasachstan	RO	Rumänien		
CZ	Tschechische Republik	LC	St. Lucia	RU	Russische Föderation		
DE	Deutschland	LI	Liechtenstein	SD	Sudan		
DK	Dänemark	LK	Sri Lanka	SE	Schweden		
EE	Estland	LR	Liberia	SG	Singapur		

INTERNATIONAL SEARCH REPORT

b ational Application No
PCT/DE 98/01922

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L9/32 H04Q7/38

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 447 380 A (TELEFONAKTIEBOLAGET L M ERICSSON) 18 September 1991 see column 2, line 42 - column 4, line 17	1,3,4,14

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 December 1998	22/01/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Behringer, L.V.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/DE 98/01922

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0447380 A	18-09-1991	SE 465800 B	28-10-1991
		AT 121254 T	15-04-1995
		AU 638820 B	08-07-1993
		AU 7495291 A	10-10-1991
		CA 2051385 A	10-09-1991
		CN 1054868 A,B	25-09-1991
		DE 69108762 D	18-05-1995
		DE 69108762 T	24-08-1995
		DK 447380 T	24-07-1995
		ES 2073726 T	16-08-1995
		FI 102134 B	15-10-1998
		HK 101895 A	30-06-1995
		IE 67887 B	01-05-1996
		JP 4505693 T	01-10-1992
		NO 300249 B	28-04-1997
		PT 96979 A,B	30-04-1993
		SE 9000856 A	10-09-1991
		WO 9114348 A	19-09-1991
		US 5390245 A	14-02-1995
		US 5282250 A	25-01-1994
		US 5559886 A	24-09-1996

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/DE 98/01922

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 6 H04L9/32 H04Q7/38

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 6 H04L H04Q

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	EP 0 447 380 A (TELEFONAKTIEBOLAGET L M ERICSSON) 18. September 1991 siehe Spalte 2, Zeile 42 - Spalte 4, Zeile 17	1,3,4,14

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
15. Dezember 1998	22/01/1999

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Behringer, L.V.

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlich..gen, die zur selben Patentfamilie gehören

Ir. ...tionales Aktenzeichen
PCT/DE 98/01922

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
EP 0447380 A	18-09-1991	SE 465800 B	28-10-1991
		AT 121254 T	15-04-1995
		AU 638820 B	08-07-1993
		AU 7495291 A	10-10-1991
		CA 2051385 A	10-09-1991
		CN 1054868 A,B	25-09-1991
		DE 69108762 D	18-05-1995
		DE 69108762 T	24-08-1995
		DK 447380 T	24-07-1995
		ES 2073726 T	16-08-1995
		FI 102134 B	15-10-1998
		HK 101895 A	30-06-1995
		IE 67887 B	01-05-1996
		JP 4505693 T	01-10-1992
		NO 300249 B	28-04-1997
		PT 96979 A,B	30-04-1993
		SE 9000856 A	10-09-1991
		WO 9114348 A	19-09-1991
		US 5390245 A	14-02-1995
		US 5282250 A	25-01-1994
		US 5559886 A	24-09-1996